

ABSTRACT

One aspect of the present invention establishes a session key by a receiving unit R transmitting a plurality of quantities for storage in a public repository. A sending unit S:

1. retrieves the plurality of quantities; and
2. computes and transmits to the unit R a plurality of sender's quantities.

The unit R then:

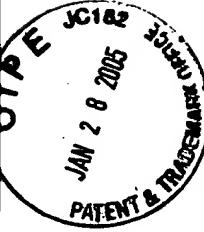
1. computes and transmits to the unit S at least one receiver's quantity; and
2. computes the session key.

The unit S, using the receiver's quantity, computes the session key.

Another aspect provides a digital signature. Before transmitting a signed message, the unit S stores a plurality of quantities in the public repository. A unit R, that receives the message and the digital signature, verifies their authenticity by:

1. retrieving the quantities from the repository;
2. using the digital signature and the quantities, evaluates expressions in at least two (2) different relationships; and
3. verifies the digital signature upon finding equality between evaluation results.

Total Words 150



Ref. US 5,581,616  
Crandall '616

Claim Text

<p>40. In a protocol for communication in which a sending unit <b>S</b> transmits onto the communication channel <b>I</b> a message "M" together with a digital signature, and, wherein before transmitting the message <b>M</b> and the digital signature, <b>the sending unit <b>S</b></b> transmits for storage in a publicly accessible repository <b>a plurality of public quantities</b>, a method by which a receiving unit <b>R</b> that receives the message <b>M</b> and the digital signature verifies the authenticity of digital signature comprising the steps performed by the receiving unit <b>R</b> of:</p> <p>a. retrieving <b>the plurality of public quantities</b> from the publicly accessible repository,</p>	<p>Disclosed in the reference.</p> <p>1. The sender computes a single quantity, <b>ourPub</b>, <u>a particular x-coordinate on the elliptic curve</u>. 2. The sender publishes the single quantity <b>ourPub</b>, by storing it into a public source 813. See column 7, line 58 through column 8, line 16.</p> <p><b>a plurality of public quantities</b>,</p> <p>the message <b>M</b> and the digital signature verifies the authenticity of digital signature</p> <p>Hasher 1206 of the encryption/decryption means 1204 of receiver 1202 <u>receives only a single quantity x-coordinate, "ourPub," from the public source 813</u>. See column 19 at lines 34 through 44.</p>
---	--

## Claim Text

Ref. US 5,581,616  
Crandall '616

b. using the digital signature and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships; and

One expression is evaluated using:  
1. only one part, i.e.  $P$ , of the digital signature  $(u, P)$ ;  
2. the ciphertext message  $C$ ; and  
3. the single quantity  $ourPub$ , i.e. a particular  $x$ -coordinate on the elliptic curve, received from the public source 813.

Hasher 1206 receives the ciphertext message  $C$  and point  $P$  on the elliptic from nonsecure channel 816 via line 1210, and  $ourPub$  from source 813 via line 1218.  
Hasher 1206 outputs point  $R$  to comparator 1208 via line 1214. See column 19, lines 40 through 44.

c. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

1. The comparator 1208 receives and compares:  
1. Q, which is computed by the elliptic multiplier 806 without using any quantity received from the public source 813; and
2. R, which is computed using ourPub which the Hasher receives from the public source 813.

The elliptic multiplier 806 of the receiver 1202 receives point  $u$  from the nonsecure channel 816. The elliptic multiplier 806 generates point  $Q$  and provides it to comparator 1208. Hasher receives the ciphertext message  $C$  and point  $P$  from the nonsecure channel 816 and the purported senders public key  $ourPub$  from source 813 and generates point  $R$ , which it provides to comparator 1208. Comparator 1208 compares points  $Q$  and  $R$  and if they match, the signature is assumed to be valid. See column 20, lines 27 through 37.

- 1) Using the  $u$  part of the signature, compute the point

$$Q = u^{\circ}(X_1/1)$$

See column 26 at lines 53 through 55.